UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

C. MARIO JARAMILLO, individually and on behalf of all others similarly situated, *Plaintiff,* *v.* AT&T Inc., *Defendant.*	Case No. 3:24-cv-761 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff C. Mario Jaramillo ("Plaintiff"), individually and on behalf of all others similarly situated ("the Class" and "Class Members"), upon personal knowledge of the facts pertaining to himself and upon information and belief as to all other matters, by and through his counsel, hereby brings this Class Action Complaint against Defendant AT&T, Inc. ("AT&T" or "Defendant").

INTRODUCTION

1. In or about March 2024, Defendant AT&T admitted that it lost control over its current and former customers' highly sensitive personal information in a data breach perpetrated by cybercriminals (the "Data Breach").

2. The Data Breach exposed the personal information of an estimated total of 73 million customers. Upon information and belief, this information includes full names, email addresses, mailing phone numbers, dates of birth, and Social Security numbers, as well as AT&T account numbers and AT&T encrypted passcodes that can be used to access AT&T customer accounts.

3. Upon information and belief, in early March of 2024, a data seller published

approximately 73 million AT&T Data Breach account records online on a known cybercrime forum on the dark web.

4. Plaintiff received notice of the AT&T Data Breach on March 30, 2024.

5. Plaintiff brings this Class Action on behalf of himself and all others harmed by AT&T's misconduct.

JURISDICTION AND VENUE

6. Jurisdiction is proper in this Court under 28 U.S.C § 1332 (diversity jurisdiction). This Court has subject matter and diversity jurisdiction over this case pursuant to 28 U.S.C. § 1332(d) because: (1) this is a class action where the amount in controversy in this class action exceeds five million dollars ($5,000,000), excluding interest and costs; (2) there are more than 100 Class members; (3) at least one member of the Class is diverse from the Defendant; and (4) the Defendant is not a government entity.

7. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

8. Defendant is headquartered and has its principal place of business in the Dallas Division of the Northern District of Texas and has sufficient minimum contacts with and intentionally avails itself of the markets in this State.

9. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims occurred within the Dallas Division of the Northern District of Texas, where AT&T is headquartered.

PARTIES

10. Plaintiff is a citizen of the State of California residing in Los Angeles, County.

11. Defendant AT&T is a corporation organized under the laws of Delaware with its principal place of business located at 208 South Akard Street, Dallas, Texas, 75202.

FACTUAL ALLEGATIONS

AT&T's Announcement

12. On March 30, 2024, Defendant issued a statement entitled "AT&T Addresses Recent Data Released on Dark Web" in which Defendant admitted that "AT&T data-specific fields" were contained in a data set released on the dark web approximately two weeks ago.[1] This information, according to AT&T, includes social security numbers and other personal information.

13. The same day, March 30, 2024, AT&T sent notice to customers (the "Data Breach Notice") stating: "We take cybersecurity very seriously and privacy is a fundamental commitment at AT&T. We have discovered that your AT&T passcode has been compromised, therefore we have proactively reset your passcode." The Data Breach Notice further stated that the Data Breach may have included: "full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number, and passcode."

14. In the Data Breach Notice, Defendant expressly encouraged its customers to be vigilant by monitoring account activity and credit reports. This is for good reason. Plaintiff and Class Members provide AT&T with their personally identifiable information ("PII") and personal information as defined by the California Consumer Privacy Act ("CCPA") ("Personal Information") when they sign up for telecommunication services. AT&T has a duty to protect this PII. When it fails, as is the case here, the impact on its current and former customers is devasting. It causes financial loss, damages credit scores, and creates emotional distress. Class Members spend hours or days sorting through finances, canceling credit cards and changing passwords to ensure that their personal information is secure.

[1] AT&T NEWSROOM, *AT&T Addresses Recent Data Set Released on Dark Web*, Mar. 30, 2024, *available at* https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (visited Mar. 31, 2024).

AT&T's Lack of Candor

15. AT&T has not been forthcoming about the nature and severity of cybersecurity events impacting its customers. Three years ago, a hacker signaled that he had stolen millions of AT&T customers' data. AT&T did not adequately warn its customers that they were in danger until years later. During this time, cybercriminals had free reign to impersonate, surveil, and defraud their unsuspecting victims.

16. Despite the Data Breach, Defendant has done very little to protect Data Breach victims. Even now, AT&T is offering victims only minimal credit monitoring services, if any.

17. Defendant failed to adequately safeguard Data Breach victims' Personal Information allowing cybercriminals to access this wealth of priceless information *for years* before AT&T warned Class Members to be on the lookout.

18. Defendant had an obligation created by reasonable industry standards, common law, and representations to Data Breach victims to keep their personal information confidential and to protect the information from unauthorized access.

19. Plaintiff and other Data Breach victims provided their PII to Defendant with the reasonable expectations and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

20. Because the Data Breach was an intentional hack by cybercriminals seeing information of value that they could exploit, victims are at imminent risk of severe identity theft and exploitation.

21. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from AT&T's failures to safeguard his

PII and Personal Information, especially his Social Security number, being placed in the hands of unauthorized third parties, including strangers and possibly criminals.

22. Plaintiff has a continuing interest in ensuring that his PII and Personal Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches and leaks.

23. Defendant owed a duty to Plaintiff and the Data Breach victims whose PII and Personal Information was entrusted to Defendant to disclose in a timely and accurate manner when data breaches occurred.

24. Defendant owed a duty of care to Plaintiff and the Data Breach victims because they were foreseeable and probable victims of any inadequate data security practices.

25. Defendant knew or should have known that Defendant's computer and/or electronic systems were targets for theft and other cybersecurity attacks because the warning signs were readily available and accessible via the Internet.

26. Today, a person's PII and Personal Information can be worth more than $1,000 on the dark web. For example, upon information and belief, online banking login information costs on average $100, and $150 if the bank account has a minimum of $100 in the account. Upon information and belief, full credit card details and associated data costs between $10 and $100.

27. This Data Breach has and will lead to further devasting financial and personal losses to Data Breach victims. As a direct and proximate result of the Data Breach, Plaintiff and the Data Breach victims have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Data Breach victims now have to spend time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including but not limited to placing "freezes" with the credit reporting agencies, contacting their

financial institutions, closing or modifying financial accounts, and reviewing and addressing unauthorized activity for years to come.

28. Plaintiff and Data Breach Victims have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

i. Trespass, damage to and theft of their personal property, including PII and Personal Information;

ii. Improper disclosure of their PII or Personal Information;

iii. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII or Personal Information being placed in the hands of criminals and having been already misused;

iv. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

v. Loss of privacy suffered as a result of the Data Breach;

vi. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

vii. Ascertainable losses in the form of deprivation of the value of customers' PII or Personal Information for which there is a well-established and quantifiable national and international market;

viii. The loss of use of and access to their credit, accounts, and/or funds;

ix. Damage to their credit due to fraudulent use of their PII or Personal Information; and

x. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

Social Security Numbers Are Particularly Valuable

29. AT&T has admitted that Class Members' Social Security numbers were included in the Data Breach.

30. Social Security numbers are among the worst kind of PII/Personal Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[2]

31. It is incredibly difficult to change a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

32. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to

[2] SOCIAL SECURITY ADMINISTRATION, *Identity Theft and Your Social Security Number*, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 31, 2024).

change—Social Security number, driver's license number, name, and date of birth. Moreover, even once changed, these pieces of identifying information can and will still match some existing databases used to verify identity, enabling continuing acts of identify theft.

33. Among other forms of fraud, identity thieves may illicitly obtain driver's licenses, employment, government benefits (including tax refunds), medical services, and housing; they may even facilitate the provision of false information to police.

34. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII/Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[3]

35. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and Personal Information of Plaintiff and Class Members, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

36. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will

[3] GOVERNMENT ACCOUNTABILITY OFFICE, *Report to Congressional Requesters*, at 29 (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited Mar. 31, 2024).

continue to incur such damages in addition to any fraudulent use of their PII.

37. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s) and thus the significant number of individuals who would be harmed by the exposure of unencrypted data.

38. According to the FTC, identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[4] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[5]

39. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be overstated.[6] "A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identity theft: 74 percent of respondents reported feeling stressed[,] 69 percent reported feelings of fear related to personal financial safety[,] 60 percent reported anxiety[,] 42 percent reported fearing for the financial security of family members[, and] 8 percent reported feeling suicidal."[7]

---

[4] FEDERAL TRADE COMMISSION, *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), *available at* https://www.justice.gov/usao-wdmi/file/764151/dl (visited Mar. 31, 2024).

[5] *See generally id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. §603.2(a). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 16 C.F.R. §603.2(b)

[6] Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, LIFELOCK BY NORTON (Feb. 4, 2021), *available at* https://www.lifelock.com/learn-identity-theft-resources-lasting-effects-of-identity-theft.html (visited Mar. 31, 2024).

[7] *Id.* (citing IDENTITY THEFT RESOURCE CENTER, *Identity Theft: The Aftermath 2016*, *available at* https://web.archive.org/web/20171113093940/https://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf (visited Mar. 31, 2024)).

40. More recently, the FTC released an updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

41. The FTC has brought enforcement actions against businesses for failing to protect consumers' PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. § 45.

42. The United States government and privacy experts acknowledge that it may take much time for identity theft to come to light and be detected because identity thieves may wait years before using the stolen data.

43. Because the information Defendant allowed to be compromised and taken is of such a durable and permanent quality (*i.e.*, name, address, date of birth, and Social Security number), the harms to Plaintiff and the Class will continue and increase, and Plaintiff and the Class will continue to be at substantial risk for further imminent and future harm.

44. Plaintiff and Class Members have suffered real and tangible losses, including but not limited to, the loss in the inherent value of their PII, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of discovery in this case.

45. Despite Defendant's failure to protect Plaintiff's and Class Members' PII/Personal Information and the resulting harm Defendant has only offered to provide Plaintiff and Class Members with one year of credit monitoring.

Plaintiff Jaramillo's Experience

46. Plaintiff Jaramillo was required to provide and did provide his PII and Personal

Information in connection with obtaining services provided by Defendant. The PII and Personal Information included, but was not limited to, his name, address, email address, Social Security number, and date of birth.

47. Plaintiff typically takes measures to protect his PII and Personal Information and is very careful about sharing his PII and Personal Information.

48. Plaintiff stores any documents containing his PII and Personal Information in a safe and secure location. He diligently chooses unique usernames and passwords for his online accounts.

49. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach.

50. As a result of the Data Breach, Plaintiff must monitor his accounts and credit scores and has sustained emotional distress. Plaintiff will need to spend additional time and effort opening new accounts. Because of the Data Breach, Plaintiff will have time taken from other obligations.

51. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

52. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

53. Plaintiff faces imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and Personal Information, especially his Social Security number, being placed in the hands of criminals.

54. As a result of the Data Breach, Plaintiff is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come. To date, Defendant

failed to either adequately protect Plaintiff and Class Members or to compensate them for their injuries sustained in this Data Breach. The offer of identity monitoring services for a limited number of months is wholly insufficient to cover the current and future harm.

Defendant Violated the FTC Act

55. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

56. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

CLASS ACTION ALLEGATIONS

57. Pursuant to the provisions of Federal Rules of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiff seeks to bring this class action on behalf of himself and a nationwide class (the "Nationwide Class"), as well as a California subclass (collectively, the "Class"), defined as follows:

> **Nationwide Class: All persons whose PII or Personal Information was accessed and/or acquired in the data incident that is the subject of the March 2024 Data Breach Notice.**
>
> **California Subclass: All persons whose PII or Personal Information was accessed and/or acquired in the data incident that is the subject of the March 2024 Data Breach Notice.**

58. Excluded from the Class are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are Plaintiff's attorneys, including all attorneys and other employees of their law firms. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

59. Plaintiff reserves the right to modify and/or amend the Nationwide Class, including, but not limited to, creating additional subclasses, as necessary.

60. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

61. All Class Members are readily ascertainable in that Defendant has access to addresses and other contact information for all Class Members, which can be used for providing notice to Class Members.

62. ***Numerosity***. Consistent with Fed. R. Civ. P. 23(a)(1), the Nationwide Class is so numerous that joinder of all members is impracticable. While the exact number of Nationwide Class Members is unknown, upon information and belief, it is in excess of 73 million and it is almost certain that it contains at least 100 individuals.

63. ***Commonality and Predominance***. Consistent with Fed. R. Civ. P. 23(a)(2) and (b)(3), this action involves common questions of law and fact that predominate over any questions that may affect only individual Class Members. Such common questions include:

a. whether Defendant engaged in the wrongful conduct alleged in this Complaint;

b. whether Defendant's conduct was unfair, unconscionable, and/or unlawful;

c. whether Defendant failed to implement and maintain adequate and reasonable systems and security procedures and practices to protect Plaintiff's and Class Members' PII and Personal Information;

d. whether Defendant owed a duty to Plaintiff and Class Members to adequately protect their PII and Personal Information and to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

e. whether Defendant breached its duties to protect the PII and Personal Information of Plaintiff and Class Members by failing to provide adequate data security and failing to provide appropriate and adequate notice of the Data Breach to Plaintiff and Class Member;

f. whether Defendant's conduct was negligent;

g. whether Defendant knew or should have known that its computer systems were vulnerable to being compromised;

h. whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach of its systems, resulting in the loss of Plaintiff's and Class Members' PII and Personal Information;

i. whether Defendant wrongfully or unlawfully failed to inform Plaintiff and Class Members that it did not maintain data security practices adequate to reasonably safeguard Plaintiff's and Class Members' PII and Personal Information;

j. whether Plaintiff and Class Members suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);

k. whether Plaintiff and Class Members are entitled to recover damages; and

l. whether Plaintiff and Class Members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

64. ***Typicality***. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of the claims of other Class Members in that Plaintiffs, like all Class Members, had their personal data compromised, breached, and stolen in the Data Breach. Plaintiff and all Class Members were injured through the misconduct of Defendant and assert the same claims for relief.

65. ***Adequacy***. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff and his counsel will fairly and adequately protect the interests of the Class. Plaintiff is a member of the Class he seeks

to represent; is committed to pursuing this matter against Defendant to obtain relief for the Class; and has no interests that are antagonistic to, or in conflict with, the interests of other Class Members. Plaintiff retained counsel who are competent and experienced in litigating class actions and complex litigation, including privacy litigation of this kind. Plaintiff and his counsel intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

66. ***Superiority***. Consistent with Fed. R. Civ. P. 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

67. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3) because the common questions of law or fact predominate over any questions affecting individual Class Members, a class action is superior to other available methods for the fair and efficient adjudication of this controversy, and the requirements of Rule 23(a) are met.

68. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(1), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish

incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

69. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant, through its uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Defendant continues to maintain its inadequate security practices, retain possession of Plaintiff's and Class Members' PII, and has not been forced to change its practices or to relinquish PII by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Class as a whole.

70. Particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. whether Plaintiff's and Class Members' PII or Personal Information was accessed, compromised, or stolen in the Data Breach;

b. whether Defendant owed a legal duty to Plaintiff and the Class Members;

c. whether Defendant failed to take adequate and reasonable steps to safeguard the PII and Personal Information of Plaintiff and Class Members;

d. whether Defendant failed to adequately monitor its data security systems;

e. whether Defendant failed to comply with applicable laws, regulations, and industry standards relating to data security;

f. whether Defendant knew or should have known that it did not employ adequate and reasonable measures to keep Plaintiffs and Class members' PII and Personal Information secure; and

g. whether Defendant's adherence to FTC data security obligations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

COUNT 1
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

71. Plaintiff repeats and re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 70.

72. Plaintiff brings this claim on behalf of himself and the Nationwide Class.

73. Defendant required Plaintiff and Class Members to submit sensitive personal information, including their PII and Personal Information, to obtain telecommunications services. Defendant collected, stored, used, and benefited from the non-public PII and Personal Information of Plaintiff and Class Members in the provision of providing telecommunications services to Plaintiff and Class Members.

74. Plaintiff and Class Members entrusted Defendant with their PII and Personal Information and Defendant was fully cognizant of the value and importance of the PII and Personal Information and the types of harm that Plaintiffs and Class Members could and would suffer if the PII or Personal Information were wrongfully disclosed.

75. Defendant negligently created a dangerous situation by failing to take adequate and

reasonable steps to safeguard Plaintiff's and Class Members' sensitive PII and Personal Information from unauthorized release or theft.

76. Defendant owed an independent duty to Plaintiff and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII and Personal Information, and preventing the PII and Personal Information from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

77. Defendant was required to prevent foreseeable harm to Plaintiff and Class Members. Accordingly, Defendant had a duty to take adequate and reasonable steps to safeguard their sensitive PII and Personal Information from unauthorized release or theft. Defendant's duties, included, but were not limited to: (1) designing, maintaining, and testing its data security systems, data storage architecture, and data security protocols to ensure Plaintiff's and Class Members' PII and Personal Information in its possession was adequately secured and protected; (2) implementing processes that would detect an unauthorized breach of its security systems and data storage architecture in a timely and adequate manner; (3) timely acting on all warnings and alerts, including public information, regarding its security vulnerabilities and potential compromise of the PII and Personal Information of Plaintiff and Class Members; and (4) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements.

78. Defendant owed a common law duty to prevent foreseeable harm to Plaintiff and Class Members. The duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices of Defendant in its collection, storage, and use of PII and Personal Information from Plaintiff and Class Members. It was foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their PII or Personal

Information because malicious actors routinely attempt to steal such information for use in nefarious purposes.

79. Defendant's obligation to use adequate and reasonable security measures also arose because Defendant collected, stored, and used the PII or Personal Information of Plaintiff and Class Members for the procurement and provision of telecommunications services.

80. Additionally, the policy of preventing future harm weighs in favor of finding a Defendant had a duty towards Plaintiff and Class Members.

81. Defendant also owed a duty to timely disclose the material fact that its computer systems and data security practices and protocols were inadequate to safeguard users' personal, health, and financial data from theft and other misuses.

82. The injuries suffered by Plaintiff and Class Members were proximately and directly caused by Defendant's failure to follow reasonable, industry standard security measures to protect Plaintiff's and Class Members' PII and Personal Information.

83. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take additional steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

84. If Defendant had implemented the requisite, industry-standard security measures and exercised adequate and reasonable care, data thieves would not have been able to take the PII or Personal Information of Plaintiff and Class Members.

85. Defendant breached these duties through the conduct alleged here in this Complaint by, including without limitation, failing to protect the PII and Personal Information in its possession; failing to maintain adequate computer systems and allowing unauthorized access to

and exfiltration of Plaintiff's and Class Members' PII or Personal Information; failing to disclose the material fact that Defendant's computer systems and data security practices were inadequate to safeguard the PII and Personal Information in its possession from theft; and failing to disclose in a timely and accurate manner to Plaintiff and Class Members the material facts of the Data Breach.

86. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and Personal Information would not have been compromised. And, as a direct and proximate result of Defendant's failure to exercise adequate and reasonable care and use commercially adequate and reasonable security measures, the PII or Personal Information of Plaintiff and Class Members was accessed by ill-intentioned individuals who could and will use the information to commit identity or financial fraud. Plaintiff and Class Members face the imminent, certainly impending, and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

87. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII or Personal Information collected from Class Members and the harm suffered, or risk of imminent harm suffered, by Plaintiff and Class Members.

88. It was foreseeable that Defendant's failure to exercise reasonable care to safeguard the PII and Personal Information in its possession or control would lead to one or more types of injury to Plaintiff and Class Members. The Data Breach was also foreseeable given the known, high frequency of cyberattacks and data breaches in the telecommunications industry.

89. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the

inherent risks in collecting and storing PII and Personal Information, the critical importance of providing adequate security of PII and Personal Information, the current cyber scams being perpetrated on PII and Personal Information, and that it had inadequate protocols, including security protocols in place to secure the PII and Personal Information of Plaintiff and Class Members.

90. Defendant's own conduct created the foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included its failure to take the steps and opportunities to prevent the Data Breach and its failure to comply with industry standards for the safekeeping, encryption, and authorized disclosure of the PII and Personal Information of Plaintiff and Class Members.

91. Plaintiff and Class Members have no ability to protect their PII and Personal Information that was and is in Defendant's possession. Defendant alone was, and is, in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

92. As a direct and proximate result of Defendant's negligence as alleged above, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII or Personal Information;

b. Unauthorized use and misuse of their PII or Personal Information;

c. The loss of the opportunity to control how their PII and Personal Information are used;

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages and time associated with efforts expended

and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII or Personal Information being placed in the hands of criminals;

g. The continued risk to their PII and Personal Information that is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII and Personal Information in Defendant's possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

93. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security measures to safeguard the PII of Plaintiff and Class Members.

94. The FTC Act prohibits "unfair . . . practices in or affecting commerce," 15 U.S.C. § 45(a)(1), which the FTC has interpreted to include businesses' failure to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

95. Defendant solicited, gathered, and stored PII of Plaintiff and Class Members to facilitate transactions that affect commerce.

96. Defendant's violation of the FTC Act (and similar state statutes) constitutes negligence.

97. Plaintiff and Class Members are within the class of persons that the FTC Act (and similar state statutes) were intended to protect.

98. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act (and similar state statutes), seeks to prevent. The FTC has pursued enforcement actions against businesses which, as a result of their failure to employ adequate and reasonable data security measures, caused the same harm as that suffered by Plaintiff and Class Members.

99. As a direct and proximate result of Defendant's violations of the above-mentioned statutes (and similar state statutes), Plaintiff and Class Members have suffered, and continue to suffer, damages arising from the Data Breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT II
Unjust Enrichment

100. Plaintiff incorporates by reference the allegations contained in paragraphs 1 through 99 as if fully set forth herein.

101. Plaintiff and class members conferred a monetary benefit on AT&T in the form of monies or fees paid for services from AT&T. AT&T had knowledge of this benefit when it accepted the money from Plaintiff and the class members.

102. The monies or fees paid by the Plaintiff and class members were supposed to be used by AT&T, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and class members.

103. AT&T failed to provide adequate security, safeguards, and protections to the personal data of Plaintiff and class members, and as a result the Plaintiff and class overpaid AT&T

as part of services they purchased.

104. AT&T failed to disclose to Plaintiff and members of the class that its computer systems and security practices were inadequate to safeguard users' and former users' personal data against theft.

105. Under principles of equity and good conscience, AT&T should not be permitted to retain the money belonging to Plaintiff and class members because AT&T failed to provide adequate safeguards and security measures to protect Plaintiff's and class members' PII and Personal Information that they paid for but did not receive.

106. AT&T wrongfully accepted and retained these benefits to the detriment of Plaintiff and class members.

107. AT&T's enrichment at the expense of Plaintiff and class members is and was unjust.

108. As a result of AT&T's wrongful conduct, as alleged above, Plaintiff and the class are entitled under the unjust enrichment laws of all 50 states and the District of Columbia to restitution and disgorgement of all profits, benefits, and other compensation obtained by AT&T, plus attorneys' fees, costs, and interest thereon.

COUNT III
Violations of California's Unfair Competition Law
CAL. BUS. & PROF. CODE § 17200, *et seq*.
(On Behalf of Plaintiff and the California Subclass)

109. Plaintiff incorporates by reference the allegations contained in paragraphs 1 through 108 as if fully set forth herein.

110. Defendant's business practices as complained of herein violate California's Unfair Competition Law, CAL. BUS. & PROF. CODE § 17200, *et seq*. ("UCL").

111. Defendant's practices constitute "unlawful" business practices in violation of the

UCL because, among other things, they violate statutory law and the common law, including, without limitation, the California Consumer Privacy Act ("CCPA"), CAL. CIV. CODE § 1798.150, and Section 5 of the FTC Act, 15 U.S.C. § 45.

112. Defendant's actions and practices constitute "unfair" business practices in violation of the UCL, because, among other things, the gravity of the harm to Plaintiff and the California Subclass members outweighs the utility of Defendant's conduct. This conduct includes Defendant's failure to adequately ensure the privacy, confidentiality, and security of members' data entrusted to it and Defendant's failure to have adequate data security measures in place.

113. As a result of Defendant's wrongful business practices, Plaintiff and members of the California Subclass have suffered injury in fact and lost money or property as alleged herein.

114. Defendant's wrongful business practices present an ongoing and continuing threat to Plaintiff and the California Subclass members.

115. Accordingly, Plaintiff and the California Subclass members have and will incur economic damages related to the Data Breach including loss of the benefit of their bargain with Defendant; time and money spent remedying the Data Breach; the costs of credit monitoring, purchasing credit reports, and purchasing "freezes" to prevent opening of unauthorized accounts.

COUNT IV
Violations of California's Consumer Privacy Act
CAL. CIV. CODE § 1798.150, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

116. Plaintiff incorporates by reference the allegations contained in paragraphs 1 through 115 as if fully set forth herein.

117. Defendant collects consumers' Personal Information, as defined in California Consumer Privacy Act ("CCPA"). CAL. CIV. CODE § 1798.140(o)(1). As a result, Defendant has a

duty to implement and maintain reasonable security procedures and practices to protect this personal information. As alleged herein, Defendant failed to do so.

118. Defendant AT&T is a corporation organized for the profit or financial benefit of its owners, and, on information and belief, has annual gross revenues exceeding $25 million and collects Personal Information as defined in the CCPA. CAL. CIV. CODE § 1798.140(o)(1). In addition, Defendant AT&T annually buys, receives, sells, or shares for commercial purposes the Personal Information of more than 50,000 consumers.

119. Upon information and belief, Defendant violated Section 1798.150 of the CPPA by failing to prevent Plaintiff and California Subclass members' nonencrypted and nonredacted Personal Information from unauthorized access, and exfiltration, theft, or disclosure. These failures were the result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

120. As a direct and proximate result of Defendant's conduct, Plaintiff and the California Subclass members' Personal Information, including names, dates of birth and Social Security numbers, was subjected to unauthorized access, exfiltration, theft, or disclosure.

121. On information and belief, Plaintiff alleges that this Personal Information was not encrypted or redacted in the format accessed during the Data Breach.

122. Plaintiff and the California Subclass members seek injunctive or other equitable relief to ensure Defendant hereafter adequately safeguards customers' Personal Information by implementing reasonable enhanced security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' Personal Information, including that of

Plaintiff and the California Subclass. These individuals have an interest in ensuring that their Personal Information is reasonably protected.

123. On March 31, 2024 Counsel for Plaintiff mailed a notice letter to Defendant's registered service agent as required under the California Consumer Privacy Act. CAL. CIV. CODE § 1798.150(b). Assuming Defendant cannot cure the Data Breach within 30 days, and Plaintiff believes any such cure is not possible under these facts and circumstances, Plaintiff will amend this complaint to seek actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Subclass as authorized by the CCPA.

RELIEF REQUESTED

WHEREFORE, Plaintiff, individually and on behalf of the proposed Nationwide Class and California Subclass, respectfully requests the following relief:

a. An order certifying this case as a class action on behalf of the Nationwide Class and California Subclass, defined above, appointing Plaintiff as Class representative of each and appointing the undersigned counsel as Class counsel of each;

b. A mandatory injunction directing Defendant to adequately safeguard Plaintiff and the Class's PII and Personal Information by implementing improved security procedures and measures as outlined above;

c. An award of other declaratory, injunctive, and equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

d. An award of restitution and compensatory, consequential, and general damages to Plaintiff and Class Members, including nominal damages as allowed by law in an amount to be determined at trial or by this Court;

e. An award of actual or statutory damages to Plaintiff and Class Members in an amount to be determined at trial or by this Court;

f. An award of reasonable litigation expenses and costs and attorneys' fees to the extent allowed by law;

g. An award to Plaintiff and Class Members of pre- and post-judgment interest, to the extent allowable; and

h. Award of such other and further relief as equity and justice may require.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

DATED: March 31, 2024

Respectfully submitted,

GEORGE FELDMAN MCDONALD, PLLC

David J. George (*pro hac vice* forthcoming)
Florida Bar No. 898570
Brittany L. Brown (*pro hac vice* forthcoming)
Florida Bar No. 105071
9897 Lake Worth Drive, Suite 302
Lake Worth, Florida 33467
Telephone: (561) 232-6002
Facsimile: (888) 421-4173
dgeorge@4-Justice.com
bbrown@ 4-Justice.com
eservice@4-Justice.com

Lori G. Feldman (*pro hac vice* forthcoming)
New York Bar No. 2389070
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Telephone: (917) 983-9321
Facsimile: (888) 421-4173
lfeldman@ 4-Justice.com

Janine L. Pollack (*pro hac vice* forthcoming)
New York Bar No. 041671989
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: (917) 983-2707
Facsimile: (888) 421-4173
jpollack@4-Justice.com

FOSTER YARBOROUGH PLLC

By: */s/ Patrick Yarborough*
Patrick Yarborough
Texas Bar No. 24084129
917 Franklin Street, Suite 220
Houston, Texas 77002
Telephone: (713) 331-5254
Facsimile: (713) 513-5202
Email: patrick@fosteryarborough.com

COUNSEL FOR PLAINTIFF AND THE PUTATIVE CLASS